

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-194618  
(43)Date of publication of application : 14.07.2000

(51)Int.Cl. G06F 13/00  
G06F 15/00  
G06T 7/00  
H04M 11/00  
H04M 15/00  
H04N 1/00

(21)Application number : 10-368025  
(22)Date of filing : 24.12.1998

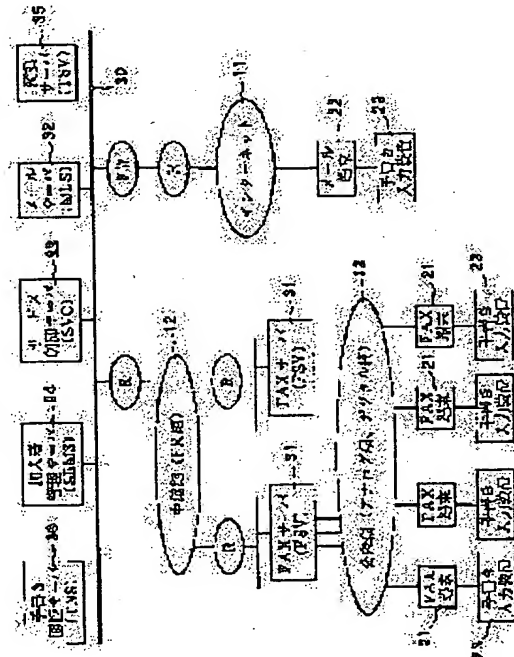
(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>  
(72)Inventor : AKAISHI DAIKI

## (54) HANDWRITE AUTHENTICATION COMMUNICATION SYSTEM AND METHOD, HANDWRITE AUTHENTICATION SERVER AND HANDWRITE INPUT DEVICE

### (57)Abstract:

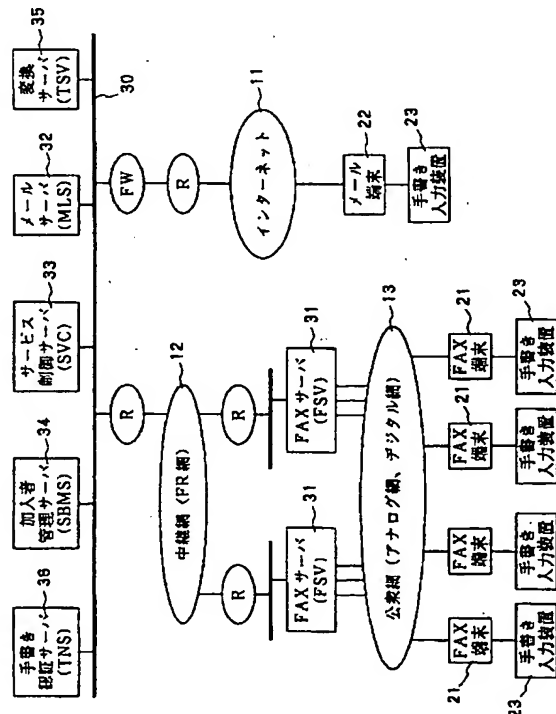
**PROBLEM TO BE SOLVED:** To improve the security of information in an information distribution step by adding an authenticating function to a communication system against the evolution of various information distribution businesses and surely authenticating an access identity when the information is transferred to an information source or the information distribution destinations.

**SOLUTION:** A service control server 33 is prepared together with a handwrite authentication server 36 which holds the handwritten signature data on a user which are initially registered and authenticates a handwritten signature. When the data are transferred from a 1st terminal (mail terminal) 22 to the 2nd terminals (Fax terminals) 21 under the control of the server 33, the server 33 instructs the server 36 to authenticate the handwrite signature data which are received from the terminal 22, controls the transfer of data based on the authentication result of the server 36 and sends the authentication result to the terminals 21 together with the picture information.



### LEGAL STATUS

[Date of request for examination] 19.12.2000  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]



## 【特許請求の範囲】

## 【請求項 1】 ネットワークと、

前記ネットワークに接続して呼処理を統括し管理するとともに前記ネットワーク上で提供されるサービスを制御するサービス制御サーバと、

前記ネットワークに接続され、利用者の初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバとを有し、

前記サービス制御サーバによる制御下で前記ネットワークに接続された第 1 の端末から前記ネットワークに接続された第 2 の端末にデータを転送する際に、前記サービス制御サーバが、前記第 1 の端末から送信された手書き署名データを前記手書き認証サーバに認証させ、その認証結果に応じて前記データの転送を制御する、手書き認証通信システム。

【請求項 2】 前記手書き認証サーバでの認証結果を前記サービス制御サーバが前記第 2 の端末に通知する、請求項 1 に記載の手書き認証通信システム。

【請求項 3】 有料情報を提供する情報サーバが接続されたネットワークと、

前記ネットワークに接続して前記情報サーバに対する呼処理を統括し管理するとともに、課金の回収処理を実行する課金回収サーバ手段と、

前記ネットワークに接続され、利用者の初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバとを有し、

前記ネットワークに接続された端末から前記利用者が前記情報サーバに格納された情報にアクセスしようとする際に、前記課金回収サーバ手段が、前記端末からの情報利用要求に添付された前記利用者の手書き署名データを前記手書き認証サーバに送信して手書き署名の認証を行わせ、前記認証で前記利用者本人であることが確認された場合には、前記情報利用要求を前記情報サーバに送信し、前記情報サーバからの情報データと課金情報とを受け取り、前記端末に前記情報データを代理提供するとともに、課金処理を実行する、手書き認証通信システム。

【請求項 4】 証明文書を提供するサーバが接続されたネットワークと、

前記ネットワークに接続して呼処理を統括し管理するとともに前記ネットワーク上で提供されるサービスを制御するサービス制御サーバと、

前記ネットワークに接続され、初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバと、

課金の回収処理を実行する課金回収サーバ手段と、を有し、

前記サービス制御サーバによる制御下で前記ネットワークに接続された端末から前記サーバに対して証明文書を請求する際に、前記サービス制御サーバが、前記端末から送信された請求者の手書き署名データを前記手書き認

証サーバに認証させ、その認証結果に応じて前記サーバに対して証明文書請求情報を転送し、前記サーバからの証明文書に添付された手書き署名データを前記手書き認証サーバに認証させ、その認証結果に応じて前記証明文書を前記端末側に送信し、前記課金回収サーバ手段に前記証明文書発行に係る課金を処理させる、手書き認証通信システム。

【請求項 5】 ネットワークを介して第 1 の端末から第 2 の端末にデータを送るための手書き認証通信方法であって、

前記ネットワークに設けられた手書き認証サーバに利用者の手書き署名データを初期登録する段階と、

前記第 1 の端末からのデータを前記ネットワーク内に保持する段階と、

前記データに添付された前記利用者の手書き署名データを前記手書き認証サーバによって認証する段階と、

前記手書き署名データを前記第 2 の端末に送ることなく、前記認証の結果に応じて、前記データの前記第 2 の端末への転送を実行する段階と、を有する手書き認証通信方法。

【請求項 6】 前記認証の結果を前記第 2 の端末に通知する、請求項 5 に記載の手書き認証通信方法。

【請求項 7】 ネットワークに接続され有料情報を提供する情報サーバを利用するための手書き認証通信方法であって、

前記ネットワークに設けられた手書き認証サーバに利用者の手書き署名データを初期登録する段階と、

前記利用者からの情報利用要求を前記ネットワーク内に保持する段階と、

前記情報利用要求に添付された手書き署名データを前記手書き認証サーバによって認証する段階と、

前記認証結果に応じて前記情報利用要求を前記情報サーバに転送する段階と、

前記ネットワークの機能により、前記情報サーバからの情報データを前記利用者に代理提供する段階と、

前記情報サーバからの課金情報を前記ネットワーク内で処理する段階と、を有する手書き認証通信方法。

【請求項 8】 ネットワークに接続され証明文書を提供するサーバに対して証明文書を請求するための手書き認証通信方法であって、

請求者からの証明請求要求を前記ネットワーク内に保持する段階と、

前記証明請求要求に添付された前記請求者の手書き署名データを前記ネットワークに設けられた手書き認証サーバによって認証する第 1 の認証段階と、

前記第 1 の認証段階での認証結果に応じて前記証明請求要求を前記サーバに転送する段階と、

前記サーバからの証明文書を前記ネットワーク内に保持する段階と、

前記証明文書に添付された手書き署名ファイルを前記手

書き証明サーバによって認証する第2の認証段階と、前記第2の認証段階での認証結果に応じて前記証明文書を前記請求者側に転送する段階と、

前記証明文書の発行に係る課金を前記ネットワーク内で処理する段階と、を有する手書き認証通信方法。

【請求項9】 手書き署名データを認証するためにネットワークに設けられる手書き認証サーバであって、前記ネットワークに対するインターフェースとなるインターフェース部と、前記ネットワークを介した情報の送受信時に情報授受者の手書き署名データの認証を行なうための認証要求部と、初期登録されている手書き署名データと送受信時の手書き署名データの比較判定を行なう認証部と、情報授受者の個人のユーザIDと事前に登録した手書き署名データを含むファイルを保持・管理する認証データベース部と、を有する手書き認証サーバ。

【請求項10】 ファクシミリ端末に接続し、手書き署名認証用の手書き署名データの入力に使用される手書き入力装置であって、前記ファクシミリ端末に対するインタフェースとなるインタフェース部と、利用者によって手書き署名がなされる手書き入力パッドと、前記利用者によって入力された手書き署名の要素解析を実行する手書き要素解析部と、前記手書き要素解析部による認識データを処理する認識データ処理部と、を有する手書き入力装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ファクシミリ通信システムを応用した通信システムに関し、特に、ネットワークにおいて発信者を認証する機能を備え、例えば情報の流通段階でのセキュリティを高めることを可能にした、手書き認証通信システム、手書き認証通信方法および手書き認証サーバに関する。

【0002】

【従来の技術】 ファクシミリ通信は、文書や画像の情報を簡便に送受信できるという特徴を有し、広く使用されるようになってきている。ファクシミリ通信では、1対1の通信のみならず、複数の宛先に一斉に情報を提供する同報通信や、ワープロ（ワードプロセッサ）文書やコンピュータ用のプログラムファイルを通信することも可能となっている。また、ファクシミリ通信を利用して、広告宣伝情報・物品販売情報・観光案内情報・イベント情報等を一般利用者に提供する情報案内サービスも実現し、拡充してきている。同報通信や時刻指定通信を効率的に実行し、かつ、大量のファクシミリ送信に対応できるようにするため、ネットワーク側にファクシミリサーバ（FAXサーバ）を設けるファクシミリ通信システムが実現している。

【0003】 図15は、最近のファクシミリ通信システムの構成例を示したものである。ここでは、ファクシミリ端末（FAX端末）間のファクシミリ画情報の通信だ

けを媒介するのではなく、パーソナルコンピュータ（パソコン：PC）などの電子メールの送受信を行うメール端末の相互間、さらには、FAX端末とメール端末の相互間で、文書や画像の送受信を行えるようにしている。そのため、公衆網（アナログ網及びデジタル網）だけでなく、インターネット（Internet）を統合して通信システムが構築されている。

【0004】 このファクシミリ通信システムでは、インターネット11、フレームリレー（FR）網などの中継網12及び公衆網13をはさんで、複数の端末（FAX端末21及びメール端末22）と機能分散処理するための複数のサーバとが配置されている。ここでは、複数のサーバとして、FAXサーバ（FSV）31、メールサーバ（MLS）32、サービス制御サーバ（SVC）33、加入者管理サーバ（SBMS）34及び変換サーバ（TSV）35等が設けられている。各FAX端末21は、アナログ網またはデジタル網の公衆網13に收容されており、公衆網13にはFAXサーバ31も接続している。FAXサーバ31は、FAX端末21からの呼受付、FAX端末21への呼配送処理を行うものであって、ルータRを介して中継網12に接続する。複数のFAXサーバ31を設け、FAXサーバ31間を中継網12で接続することにより、公衆網13に負担をかけることなく、大量のファクシミリ画情報の通信を高速に処理し伝送できるようになっている。メール端末22は、インターネット11に接続している。

【0005】 メールサーバ32、サービス制御サーバ33、加入者管理サーバ34及び変換サーバ35は、相互にバックボーン網30に接続し、また、バックボーン網30は、ルータRを介して中継網12に接続し、ファイアウォールFW及びルータRを介してインターネット11に接続している。ここでメールサーバ32は、メール端末22からの呼受付、メール端末22への呼配送処理を実行する。サービス制御サーバ33は、すべての呼処理を統括し、管理するサーバであって、各種サービスの呼処理、規制状態の把握、通信記録情報の収集を行う。加入者管理サーバ34は、サービスオーダー情報やサービスカスタム情報の保持・管理を行う。さらに、変換サーバ35は、出力端末に合わせて画情報の変換処理を行うとともに、出力端末に合わせた通知文を作成する。

【0006】 図15に示すファクシミリ通信システムにおいて実現される通信プロセスとしては、主として、FAX端末21間の通信、メール端末22間の通信、及びFAX端末21-メール端末22間の3種類の通信がある。ここでFAX端末21間の通信は、従来型のファクシミリ通信システムと同様であり、メール端末22間の通信は、インターネット上の電子メールの転送と同じである。そこで、以下では、メール端末22からFAX端末21に送信する際の手順を図16のシーケンス図により説明する。

【0007】メール端末22は、着信宛先番号を指定し、文書・画情報を添付ファイルとして、電子メールをメールサーバ32に送信する。ここではメールサーバ32のホスト名として、「fax-net.ne.jp」が指定されているものとする。

【0008】メール端末22がメールを送信する際には、宛先端末を特定するために、メールヘッダ中の「To:フィールド」欄を使用する。「To:フィールド」は、インターネット上の電子メールにおいて宛先を特定するために使用されるものであり、一般に、「ユーザ名@ドメイン名」という形式で表わされるものである。ここでは、ドメイン名としては上述のメールサーバ32のホスト名を用いることとし、ユーザ名のフィールドを用いて宛先端末を特定する。例えば、宛先となるFAX端末21の電話番号によって宛先端末を特定する電話番号指定方法では、「To:フィールド」のユーザ名部分に、サービスコード（ここでは、#263とする。）に続けて、着FAX端末の電話番号を指定する。具体的には、「To:フィールド」欄の内容を、「#263\*

（着FAX端末電話番号）@fax-net.or.jp」とする。

【0009】メール端末22からの上述のメールは、宛先のドメイン名として「fax-net.ne.jp」が指定されているので、インターネット11を介してメールサーバ32に到達し、メールサーバ32は、添付ファイルの形式で送られてきた画情報を一時的に蓄積するとともに、サービス制御サーバ33に対して、SMTP（Simple Mail Transfer Protocol）形式で、発信要求指示を送信する。発信要求を受けたサービス制御サーバ33は、メール端末22からの「To:フィールド欄」の宛先情報を解析するとともに、加入契約者であるかどうかの照合（発照合）を加入者管理サーバ34に要求する。加入者管理サーバ34は、ユーザID、メールアドレス、パスワード、サービスオプション情報などから加入契約者か否かを検索し、その照合結果をサービス制御サーバ33に応答する。

【0010】サービス制御サーバ33は、加入契約登録者であることを判断すると、その後、メール端末22からの画情報の蓄積形式を揃えるために、メールサーバ32の画情報を取り出して、変換サーバ35により変換し蓄積するように制御する。すなわち、サービス制御サーバ33は、メールサーバ32に対して発信応答を通知し、メールサーバ32がこの発信応答に対して準備完了を通知すると、変換サーバ35に対して画ファイル変換要求を行う。画ファイル変換要求を受けて変換サーバ35は、サービス制御サーバ33にアクセスして変換対象の画ファイルを示したリストファイルを取り出し、メールサーバ32から変換対象の画ファイルを取り出し、取り出した画ファイルの画像フォーマットをFAX端末に適したフォーマットに変換する。その後、変換サーバ3

5は取出し応答をサービス制御サーバ33に送り、これを受けてサービス制御サーバ33は、配送処理を行うFAXサーバ31に対して、画ファイル取出し要求を送信する。

【0011】画ファイル取出し要求を受信したFAXサーバ31に対して変換サーバ35が変換後の画ファイルを配送し、FAXサーバ31は、公衆網を通して宛先に指定されたFAX端末21に、その画ファイルを画信号として配送する。その結果、FAX端末21では、メール端末22からの文書・画像が、ファクシミリ画として受信される。

【0012】上述した一連の処理の終了により画信号の配送が終了したら、FAXサーバ31はサービス制御サーバ33に対して処理結果として端末配送完了を通知し、サービス制御サーバ33は、メールサーバ32に対して、送信終了の通知文の配送を指示し、これによって、メールサーバ32はその通知文を発信元のメール端末22に配送する。

【0013】

【発明が解決しようとする課題】以上の通信処理フローにより、メール端末22からインターネット11や公衆網13を経由して、FAX端末21に文書・画情報を送受信できる。このような通信システムでの送信側のメール端末22での情報提供者の特定は、加入者管理サーバ34内のデータベースを用いて契約者の「ユーザID」と「パスワード」を照合するにより行なっている。しかしながら、このような特定は、厳密には、発信人個人すなわち情報提供者個人を特定するものではなく、メール端末22が加入契約者（の端末）であることを特定しているに過ぎない。同様に、FAX端末21では電話番号がIDに相当するが、FAX端末21での送受信者個人を特定しているのではなく、契約した電話番号を特定しているに過ぎない。このため、メール端末22あるいはFAX端末21等で契約者と利用者本人とが不一致の場合が生じ、契約者になりすまして使用することが可能になる。

【0014】インターネットの進展により、ネットワークを介した情報流通の機運が高まっているが、情報や通信の信頼性を高めるには、情報の不適切な流出の防止の管理や、情報源の確実な特定などに、現行以上の技術性能が要求される。例えば、流通業でのマークシートによる受発注システムでは、契約授受での確実な取引決済として、受発注者の特定が要請されつつあり、また、電子ショッピングでの契約決済での本人の特定等が要請されつつある。現状では、本人認証は、数字や英文字との組合せ等により行なうパスワードの指定により行っているが、ネットワークを介した本人認証に関し、さらなる代替手段の実現が望まれている。

【0015】最近では、電子商取引などのシステムにおいて、公開鍵暗号方法に基づき、第三者認証証明機関

(CA ; Certification Authority、例えば米国のベリサイン社など) によって認証された公開鍵を使用するデジタルID認証方式が実験的に導入されている。しかしながらこの方式の場合、秘密鍵の保存や公開鍵の取得等の複雑さがある。

【0016】人間の生物学的な特徴、身体的な特徴を用いることにより、情報授受者個人を特定する技術としては、多種のものがある。目の網膜にある毛細血管の模様や瞳孔周辺の筋肉の模様である虹彩を分析する方法、指紋を読み取る方法がその代表例として知られているが、生物学的特徴を情報化するための小型の入力端末が入手困難であること、個人の特徴的情報収集での照明や皮膚条件などの環境条件での整備が必要であるなどの課題がある。

【0017】生物学的な特徴として、手書き署名を用いる認証システムがいくつか実用化されている。例えば、入力デバイスおよび専用サーバの設置による社内LAN（ローカルエリアネットワーク）システムでの手書き認証システムとして、CADIX社（株式会社キャディックス）が「VIPSTATION」の商品名で提案した手書き電子決済が可能なシステムがある。このシステムでは、手書き署名者本人であることを認証して社内LANへのアクセスを可能にし、あるいは、電子稟議書等への決済を可能にしたものである。

【0018】さらに、特開平9-81518号、特開平9-81519号、特開平9-81520号の各公報には、利用者の認証のために、タブレットなどの入力装置に対して手書き入力された署名を用いるシステムが開示されている。このシステムでは、利用者に対してサービスを提供するアプリケーションサーバとは別に照合サーバを設けている。このシステムにおいてクライアント端末側のユーザがアプリケーションサーバにアクセスした場合には、アプリケーションサーバがアプリケーションキーの入力を要求するメッセージをユーザ側に返し、ユーザがこの要求を受けてキーをアプリケーションサーバに送信したら、アプリケーションサーバが照合サーバに照合準備要求を送り、この照合準備要求に基づいて照合サーバはメッセージIDや暗号キーを作成してアプリケーションサーバに送る。そして、アプリケーションサーバは、メッセージIDや暗号キーを添付してユーザ側に署名入力要求を送り、ユーザ側では署名入力プログラムが起動し、ユーザによる手書き署名が入力され、この署名データが、キーデータ、メッセージIDともに、アプリケーションサーバを介してあるいは直接、照合サーバに送られる。照合サーバは署名データに含まれる手書き署名を認証し、その結果をアプリケーションサーバに送信する。アプリケーションサーバは、照合サーバから通知された結果に基づいて、次のアクションを実行する。

【0019】しかしながら、上述した手書き認証システムや、特開平9-81518号、特開平9-81519

号、特開平9-81520号の各公報に開示のシステムは、通信手順が複雑であるとともに、手書き署名を入力して照合サーバ側に送るための特別のプログラムをユーザ端末側に必要とするという問題点を有する。また、FAX端末などから入力された手書き署名を認証することができないという問題点も有する。さらに、社会的インフラストラクチャーである公衆通信システム、公衆通信ネットワーク自体に認証機能を持たせる場合にも、適用しにくいという問題点がある。

10 【0020】手書き署名による認証の場合、正当な手書き署名データとの比較を行うため、認証サーバに本人の手書き署名を前もって登録（初期登録）しておく必要がある。公衆通信システム、公衆通信ネットワーク自体に手書き署名の認証機能を持たせることは、分散している情報提供者等のそれぞれに手書き署名の初期登録データを蓄積する必要がなくなることであり、これにより、利用者の手間が省けることになる。さらに、公衆通信システム、公衆通信ネットワーク自体に手書き署名の認証機能を持たせることにより、情報提供者側には利用者の手書き署名データが送られないので、不適切な運用をする情報提供者から手書き署名データが流出することを防ぐことになり、セキュリティの大幅な向上が期待される。

【0021】本発明は、多様な情報流通ビジネスの展開に備え、通信システムに認証機能をもたせ、情報源や情報配布先との情報授受の段階での確実なアクセス本人の認証を実現することにあり、あらゆる情報流通段階での情報へのセキュリティを高めることを目的とするものである。

30 【0022】

【課題を解決するための手段】本発明は、通信システムへの情報授受の段階での本人の特定のための本人認証機能を設けたもので、個人を特定するために生物学的な特徴行為を要請し、その行為を情報化し、それを蓄積し、管理するサーバを通信システム内に配置したことを主要な特徴としている。具体的には、個人の生物学的な特徴行為として、個人名などの手書き署名行為を要請し、その手書き署名行為を入力装置により手書き署名データとして情報化し、その手書き署名データを事前登録したのち、送受信アクセスのたびに手書き署名行為を行ない、事前登録とのデータファイルの比較検討を行ない、手書き署名者を認証したのち、認証結果を相手側に送信するものである。

40 【0023】すなわち本発明の第1の手書き認証システムは、ネットワークと、ネットワークに接続して呼処理を統括し管理するとともにネットワーク上で提供されるサービスを制御するサービス制御サーバと、ネットワークに接続され、利用者の初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバとを有し、サービス制御サーバによる制御下でネット

ワークに接続された第1の端末からネットワークに接続された第2の端末にデータを転送する際に、サービス制御サーバが、第1の端末から送信された手書き署名データを手書き認証サーバに認証させ、その認証結果に応じてデータの転送を制御する。この手書き認証通信システムでは、手書き認証サーバでの認証結果をサービス制御サーバが第2の端末に通知するようにしてもよい。

【0024】本発明の第2の手書き認証通信システムは、有料情報を提供する情報サーバが接続されたネットワークと、ネットワークに接続して情報サーバに対する呼処理を統括し管理するとともに、課金の回収処理を実行する課金回収サーバ手段と、ネットワークに接続され、利用者の初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバとを有し、ネットワークに接続された端末から利用者が情報サーバに格納された情報にアクセスしようとする際に、課金回収サーバ手段が、端末からの情報利用要求に添付された利用者の手書き署名データを手書き認証サーバに送信して手書き署名の認証を行わせ、認証で利用者本人であることが確認された場合には、情報利用要求を情報サーバに送信し、情報サーバからの情報データと課金情報とを受け取り、端末に情報データを代理提供するとともに、課金処理を実行する。

【0025】本発明の第3の手書き認証通信システムは、証明文書を提供するサーバが接続されたネットワークと、ネットワークに接続して呼処理を統括し管理するとともにネットワーク上で提供されるサービスを制御するサービス制御サーバと、ネットワークに接続され、初期登録された手書き署名データを保持して、手書き署名の認証を行う手書き認証サーバと、課金の回収処理を実行する課金回収サーバ手段と、を有し、サービス制御サーバによる制御下でネットワークに接続された端末からサーバに対して証明文書を請求する際に、サービス制御サーバが、端末から送信された請求者の手書き署名データを手書き認証サーバに認証させ、その認証結果に応じてサーバに対して証明文書請求情報を転送し、サーバからの証明文書に添付された手書き署名データを手書き認証サーバに認証させ、その認証結果に応じて証明文書を端末側に送信し、課金回収サーバ手段に証明文書発行に係る課金を処理させる。

【0026】本発明の第1の手書き認証通信方法は、ネットワークを介して第1の端末から第2の端末にデータを送るための手書き認証通信方法であって、ネットワークに設けられた手書き認証サーバに利用者の手書き署名データを初期登録する段階と、第1の端末からのデータをネットワーク内に保持する段階と、データに添付された利用者の手書き署名データを手書き認証サーバによって認証する段階と、手書き署名データを第2の端末に送ることなく、認証の結果に応じて、データの第2の端末への転送を実行する段階と、を有する。この手書き認証

通信方法では、認証の結果を第2の端末に通知するようにしてもよい。

【0027】本発明の第2の手書き認証通信方法は、ネットワークに接続され有料情報を提供する情報サーバを利用するための手書き認証通信方法であって、ネットワークに設けられた手書き認証サーバに利用者の手書き署名データを初期登録する段階と、利用者からの情報利用要求をネットワーク内に保持する段階と、情報利用要求に添付された手書き署名データを手書き認証サーバによって認証する段階と、認証結果に応じて情報利用要求を情報サーバに転送する段階と、ネットワークの機能により、情報サーバからの情報データを利用者に代理提供する段階と、情報サーバからの課金情報をネットワーク内で処理する段階と、を有する。

【0028】本発明の第3の手書き認証通信方法は、ネットワークに接続され証明文書を提供するサーバに対して証明文書を請求するための手書き認証通信方法であって、請求者からの証明請求要求をネットワーク内に保持する段階と、証明請求要求に添付された請求者の手書き署名データを前記ネットワークに設けられた手書き認証サーバによって認証する第1の認証段階と、第1の認証段階での認証結果に応じて証明請求要求を前記サーバに転送する段階と、サーバからの証明文書を前記ネットワーク内に保持する段階と、証明文書に添付された手書き署名ファイルを手書き証明サーバによって認証する第2の認証段階と、第2の認証段階での認証結果に応じて証明文書を請求者側に転送する段階と、証明文書の発行に係る課金をネットワーク内で処理する段階と、を有する。

【0029】さらに本発明の手書き認証サーバは、手書き署名データを認証するためにネットワークに設けられる手書き認証サーバであって、ネットワークに対するインターフェースとなるインターフェース部と、ネットワークを介した情報の送受信時に情報授受者の手書き署名データの認証を行なうための認証要求部と、初期登録されている手書き署名データと送受信時の手書き署名データの比較判定を行なう認証部と、情報授受者の個人のユーザIDと事前に登録した手書き署名データを含むファイルを保持・管理する認証データベース部と、を有する。

【0030】本発明の手書き入力装置は、ファクシミリ端末に接続し、手書き署名認証用の手書き署名データの入力に使用される手書き入力装置であって、ファクシミリ端末に対するインタフェースとなるインタフェース部と、利用者によって手書き署名がなされる手書き入力パッドと、利用者によって入力された手書き署名の要素解析を実行する手書き要素解析部と、手書き要素解析部による認識データを処理する認識データ処理部と、を有する。

【0031】



【発明の実施の形態】次に本発明の実施の形態について、図面を参照して説明する。

【0032】《個人認証ファクシミリ通信システム》図1は、本発明の好ましい実施の形態の手書き認証通信システムとしての個人認証ファクシミリ通信システムの構成を示すブロック図である。このシステムは、図15に示した従来のファクシミリ通信システムにおいて手書き認証サーバ36を配置するとともに、FAX端末21やメール端末22には、情報授受者個人の手書き署名（サイン）による生物学的な筆跡軌跡を情報処理化する手書き入力装置23を増設し、端末と通信システム間での固有な処理手順により、通信システムにおける個人認証システムを構築するものである。以下、主要構成部について詳細に説明する。

【0033】(1-1)手書き認証サーバ：図2は、手書き認証サーバ（TNS）36の構成を示すブロック図である。手書き認証サーバ36は、サービス制御サーバ33に対するインターフェースとなるサービス制御サーバインターフェース部51と、送受信時に情報授受者の手書き署名データの認証を行なうための認証要求部52と、初期登録されている手書き署名データと送受信時の手書き署名データの比較判定を行なう認証部53と、情報授受者の個人のユーザIDや事前に登録した（初期登録された）手書き署名データファイルを保持・管理する認証データベース部54と、から構成されている。このような構成により、手書き認証サーバ36は、初期登録されている手書き署名データと、送受信アクセス時点での情報授受者の手書き署名による手書き署名データとについて、両者の手書き署名データから特徴量を抽出したのち比較し、同一性のある手書き署名データであれば登録者本人であることを認証し、同一性がない場合は登録者ではないとの認証を行ない、その結果をサービス制御サーバインターフェース部51を通して回答する。

【0034】(1-2)手書き入力装置：上述したように、情報授受者個人の生物学的な特徴を利用して個人を特定する技術としては、例えば、虹彩を分析する方法や指紋を読み取る方法などがあるが、小型の入力端末の入手が難しいこと、照明や皮膚条件などの環境条件での整備が必要であるなどの課題がある。そこで、本発明では、電子ペンを用いてパッドに個人名などのサインを行なう手書き署名における動的特徴要素を分析し、デジタル情報化する方法を採用した。この方法は、すでにCADIX社により開発されたものであり、署名での形状、ペン先の圧力、書き順、空中でのペン先の動き、書く速さなどを要素解析し、デジタルデータ化するものである。本発明では、手書き署名用の入力装置すなわち手書き入力装置23をFAX端末21やメール端末22と接続し、手書き署名データを通信システムで送受信することになる。

【0035】図3は、手書き入力装置23の構成を示す

ブロック図である。手書き入力装置23は、端末（FAX端末21、メール端末22、PC端末など）に対するインタフェースとなるインタフェース部55と、認識データを処理する認識データ処理部56と、手書き署名での署名の形状、ペン先の圧力、書き順、空中でのペン先の動き、書く速さなどを要素解析する手書き要素解析部57と、ユーザによって手書き署名がなされる手書き入力パッド58と、からなっている。手書き入力パッド58としては、いわゆるタブレットなどを使用することができる。この手書き入力装置23では、あらかじめ手書き要素解析部57に解析用ソフトウェアを、認識データ処理部56にデータ処理用ソフトウェアをインストールしておくことにより、情報授受者個人が手書き入力パッド58にペンによる手書き署名を行なえば、その署名文字の特徴的要素がデータとして変換され、FAX端末21またはメール端末22に送信可能となる。

【0036】なお、一般的にはパソコンで構成されるメール端末22では、ラップトップ型ないしノート型のものが普及しており、メール端末の液晶画面に手書き署名することが可能なように、メール端末に手書き入力装置を一体化させるように組み込んだメール端末を用いることも可能である。

【0037】(1-3)本実施形態の通信システムでの手書き認証処理手順の特徴：入力デバイス及び専用サーバの設置による社内LANシステムでの手書き認証システムとしては、上述したCADIX社による商品名「VIP STATION」がある。これに対し本発明の手書き認証通信システムでは、公衆通信システムを介して手書き署名データを送受信するとともに、本人の認証の結果を送信者本人ではなく受信者に通知する。さらに、手書き署名者側の端末として、公衆通信システムに接続するFAX端末やメール端末など、多種の端末を使用することができる。

【0038】(1-4)手書き認証の通信処理手順：次に、この手書き認証通信システムにおける通信処理手順について説明する。

【0039】（初期登録手順）認証を行う前に、初期登録として、あらかじめ本人の手書き署名データを手書き認証サーバ（TNS）36の手書き署名データベース部54に登録しておく必要がある。図4は、この初期登録の手順を示すシーケンス図である。

【0040】FAX端末21またはメール端末22に対して接続する手書き入力装置23に、手書き署名を解析しデジタルデータに変換する署名解析およびデータ処理用ソフトウェアをあらかじめインストールしておく。そして、この手書き入力装置23をメール端末22に接続し、手書き入力装置23にインストールされたソフトウェアの初期登録のメニューに従い、手書き入力パッド58上で個人の手書き署名（サイン）を連続して3回ほど行なう。手書き署名の試行回数は3回に限定されるも

10

20

30

40

50



のではないが、回数が少なすぎれば、署名のばらつきの影響を受けやすくなり、回数が多すぎれば、煩雑になるとともに署名データが大きくなるという問題点を生じる。そこで、一般的には、3回程度連続して手書き署名入力を行えばよいと考えられる。そして、これらの3回の署名のそれぞれに対して、手書き入力装置23は署名データファイルを作成する。ここでは、ファイル名をそれぞれ「nmaster1.svs」、「nmaster2.svs」、「nmaster3.svs」とする。

【0041】メール端末22は、通常の電子メール送信手順により、通信システムの手書き認証サーバ36への登録要求メールの送信を行う。その際のメールでの指定例を図5に示す。よく知られているようにSMTPにしたがう電子メールのデータは、メールヘッダ81とメール本文82とから構成され、メールヘッダ81には、宛先を示す「To: フィールド」や発信元を示す「From: フィールド」、そのメールの件名を示す「Subject: フィールド」が含まれているが、ここでは、「To: フィールド」の記載を、「#213\*tnsup@fax-net.ne.jp」とする。ここで「#213」は、サービス識別子であり、ここでは手書き認証サービスとする。「tnsup@fax-net.ne.jp」は、手書き認証サーバのドメイン名と初期登録のコマンドとに対応する。メール本文82には、ユーザID（1行目の#Useridの項目）とパスワード（2行目の#Passwordの項目）を記載し、また添付ファイルとしてさきの3つのファイル名を記載し、これら3つのファイルを添付ファイルとして添付する。

【0042】メールサーバ32では、添付ファイルを一時蓄積した後、サービス制御サーバ33に発信要求を行ない、サービス制御サーバ33は、サービス種類の分析を行なうとともに、加入者管理サーバ34に「ユーザID」を送って発信者が加入契約者であることを確認する（発照合要求と発照合応答）。そののち、サービス制御サーバ33は、手書き認証サーバ36に初期登録要求を行なう。

【0043】手書き認証サーバ36は、初期登録要求に対して初期登録応答をサービス制御サーバ33に返し、初期登録応答を受けたサービス制御サーバ33は、メールサーバ32に対して送信要求を行なう。するとメールサーバ32は、3個の初期登録用の添付ファイル（手書き署名データ）を手書き認証サーバ36に送信する。

【0044】手書き認証サーバ36は、ユーザIDと3個の手書き署名データの添付ファイルを手書きデータベース部54に格納する。その後、サービス制御サーバ33に登録完了を通知する。サービス制御サーバ33は、メールサーバ32に対し、登録完了の通知文をメール端末22に向けて配送するように要求し、メールサーバ32は、メール端末22に登録が完了となったことを通知する。以上のようにして初期登録が終了する。

【0045】（送受信処理手順）次に、この手書き認証通信システムにおいて、メール端末22からFAX端末21に対して画情報を送受信する際に、手書き署名によって発信者の認証を行う際の処理を説明する。図6は、この送受信の処理フローを示している。

【0046】メール端末22では、送信すべきメールのメールヘッダの「To フィールド:」に、「#213\*（相手FAX端末番号）@fax-net.ne.jp」と記載するとともに、メール端末22上での送受信処理メニューにおいて手書き入力装置23による手書き署名を行ない、その手書き署名データを添付ファイルとし、また、FAX端末21側に送信すべき画情報を添付ファイルとする。

【0047】メール端末22から、これらの添付ファイル（画情報と手書き署名データファイル）が添付された電子メールが送信されると、メールサーバ32は、そのメールを受け付け、添付ファイルを一時蓄積した後、サービス制御サーバ33に発信要求を行なう。サービス制御サーバ33は、サービス種類の分析を行なうとともに、加入者管理サーバ34に「ユーザID」を送って発信者が加入契約者であることを確認する（発照合要求と発照合応答）。そののち、サービス制御サーバ33は、手書き署名の登録確認を要求するために、手書き認証サーバ36に認証要求を送信する。

【0048】手書き認証サーバ36は、認証要求に対して認証応答をサービス制御サーバ33に返し、認証応答を受けたサービス制御サーバ33は、メールサーバ32に対して送信要求を行なう。するとメールサーバ32は、手書き署名ファイルを手書き認証サーバ36に送信する。

【0049】手書き認証サーバ36は、ユーザIDに基づいて、手書き署名データベース部54内で初期登録データを検索するとともに、今回の手書き署名データとの特徴量について同一性を比較し、認証する。その結果を認証結果通知としてサービス制御サーバ33に応答する。サービス制御サーバ33は、手書き認証サーバ36からの応答により、手書き認証の同一性があれば、登録者名を記録し、画情報送信要求をメールサーバ32に送る。これを受けてメールサーバ32は、画情報をFAXサーバ31に送信する。その際、必要に応じて、変換サーバ35において画情報の形式変換を行うものとする。また、サービス制御サーバ33は、認証結果をFAXサーバ31にも送信する。画情報と認証結果通知を受信したFAXサーバ31は、宛先となるFAX端末21に対し、画情報と認証結果を送信する。その結果、FAX端末21からは、画情報と認証結果（登録者名）とが出力される。図7は、この出力例を示したものであり、ファクシミリ受信紙の上部のいわゆるヘッダ85の部分に認証結果が記載されて出力される。本文86には、メール端末22からの画情報が記録されている。

【0050】このようにしてFAX端末21への配信が終了すると、FAXサーバ31は、受信完了通知をサービス制御サーバ33に返し、サービス制御サーバ33は、メールサーバ32に対し、受信完了の通知文をメール端末22に向けて配送するように要求し、メールサーバ32は、メール端末22に、受信が完了となったことを通知する。以上のようにして画情報の送受信が終了する。

【0051】手書き認証サーバ36での手書き署名データファイルの同一性比較において同一性が低いと判断された場合には、手書き認証サーバ36は、サービス制御サーバ33に対して非認証の応答を行ない、その結果、メールサーバ32を経由してメール端末22には「署名が違います」とのメッセージが送信される。いずれにせよ、その場合は、再度の手書き署名を行ない、添付ファイルとして送信する。手書き認証サーバ36での認証結果が非認証である限り、画情報がFAXサーバ31に送信されることはない。

【0052】なお、送信側の手書き認証結果を受信側に通知したくない場合には、「Toフィールド:」の先頭部にオプション識別子を設け、サービス制御サーバでこの識別子を識別するようにすればよい。

【0053】(登録変更手順)次に、初期登録した手書き署名データの登録変更をする場合の処理を説明する。登録変更を行う際には、手書き入力装置23をメール端末22に接続するとともに、手書き入力装置23でのメニューから「登録変更」を選択し、初期登録と同様に手書き署名を3回行ない、初期登録のときと同様の添付ファイル名称(「nmaster1.svs」,「nmaster2.svs」,「nmaster3.svs」)とし、メールヘッダの「Toフィールド:」を「#213\*tnsch@fax-net.ne.jp」として、メール端末22からメールを通信システム側に送信する。すると、初期登録のときとはほぼ同様の手順で、サービス制御サーバ33、加入者管理サーバ34、手書き認証サーバ36に対するアクセスが行われ、変更が完了すれば、登録完了通知がメール端末22に送信される。

【0054】以上の通信処理手順により、送信端末でのアクセス者の特定を受信側端末に通知することができる。本実施の形態の手書き認証通信システムでは、このような認証通知機能を通信システムに設けることにより、よりセキュリティの高い通信システムが構築できる。

【0055】《認証機能付受発注情報処理システム(マークシート受発注システム)》従来から、OCR(光学的文字読み取り装置)によるマークシート(帳票)処理システムにファクシミリ通信システムを融合させた情報処理システムが開発されており、商品の受発注を効率的に処理できるシステムとして普及しつつある。この受発注システムでは、発注者側が発注情報を入力用帳票に数

字またはマークで記入し、それをファクシミリ装置で読み取らせてその画情報を受注センタ側へ送信し、一方、受注センタ側では、ディスク装置等により商品種別を予め格納しておいて受信した入力帳票の画情報を解析することにより、受注確認を行なうようになっている(例えば、特開平7-115525号公報等)。

【0056】このような受発注情報通信処理システムにおいては、発注者の正確な身元確認が要請されている。身元確認の方法としては、発信者IDによる事前登録と受注時の入力による確認方法(特開平6-215180号公報)や、ICカードによる発信者の特定などの方法(特開平7-115525号公報等)が提案されている。しかしながら、発信者IDやICカードでの身元確認では、実際に受注した本人かどうかは厳密には不明であり、より確実な受注者の特定方法が要請されている。

【0057】(システム構成)図8は、本発明の手書き認証通信システムを適用した認証機能付き受発注情報処理システムの構成を示したブロック図である。

【0058】多数の発注者を含む発注側は、手書き署名データ入力用の手書き入力装置23がそれぞれ接続された複数のFAX端末21が公衆網13と結合した構成となっている。FAX端末21としては、BFT(バイナリ・ファイル・トランスファ)機能を有しており、バイナリファイルの転送も可能なFAX端末が使用される。公衆網13には、その一部として、FAXサーバ31、サービス制御サーバ33、加入者管理サーバ34および手書き認証サーバ36などのサーバ群が設けられている。これらのサーバ群の機能は、既に説明した通りである。一方、多数の発注データを受信・集計し、受注データを作成する受注センタには、PCサーバ41が設置されている。このPCサーバ41は、発注帳票の画情報の解析・蓄積機能と、発注会員データベース機能と、商品種別のマスター情報格納機能と、全受注情報の集計機能を有し、専用線40によって公衆網13側に結合している。実際には、受注センタの規模が大きければ、PCサーバ41は、受発注データの処理と管理を行なう複数のサーバ群で構成されることになろう。なお、FAX端末21はデータの送信元である第1の端末であり、PCサーバ41は、データの受け手となる第2の端末に相当する。

【0059】手書き認証サーバ36の構成は図2に示した通りであり、手書き入力装置23の構成は図3に示した通りである。

【0060】(処理手順)このような受発注通信処理システムでの基本的な通信処理手順は、図9に示すようになる。

【0061】発注側では、受注センタから送られた帳票に発注情報を記入するとともに、パスワードを入力し、また、手書き入力装置23によって手書き署名を行ない、手書き署名データファイルを添付して、発注側に送

10

20

30

40

50

信する。この送信データはまず F A Xサーバ 31 によって受け付けられ、F A Xサーバ 31 からサービス制御サーバ 33 に発信要求が行われて、サービス制御サーバ 33 と加入者管理サーバとの間で発照合対応を実行することにより、公衆網側での加入者確認が行われる。その後、サービス制御サーバ 33 が署名ファイル送信要求を F A Xサーバ 31 に送信し、これを受けて F A Xサーバ 31 が手書き署名データファイルを手書き認証サーバ 36 に送ることにより、手書き認証サーバ 36 は、送信されてきた手書き署名データファイルで事前登録者か否かの判定を行い、認証結果をサービス制御サーバ 33 に送る（認証対応）。これにより、サービス制御サーバ 33 は、帳票送信要求を F A Xサーバ 31 に送るとともに、認証結果を P Cサーバ 41 に送信する。その後、F A Xサーバ 31 が発注帳票を帳票画情報として P Cサーバ 41 に送信する。

【0062】帳票画情報を受信した受注センタの P Cサーバ 41 は、発注者データベース（D B）を照合するとともに、帳票画の文字認識を行って発注内容を確認し、受注確認書を作成する。その後、P Cサーバ 41 は、F A Xサーバ 31 を経由して、受注確認書を発注側の F A X端末 22 に送信する。すると、発注側の発注確認者は、手書き署名データファイルを添付して受注センタに返信する。再度、公衆網内での加入者確認および発注確認者の手書き認証を行ない、受注確認書を専用線を経由して受注センタの P Cサーバ 41 へ送信する。受注センタの P Cサーバ 41 は、返信されてきた受注確認書を再度、解析、認識した後、発注者ごとおよび全受注総計のリスト、ならびに発注者認証結果、発注確認者認証結果を添付して集計データを作成する。

【0063】この受発注情報通信システムでは、公衆網に設置した手書き認証サーバによって発注者の特定を行ない、その結果を受注センタ側へ通知することにより、発注者および発注確認者の個人特定が可能となった。

【0064】以上、発注者側の端末が F A X端末であるものとして受発注情報通信システムを説明したが、発注者側の端末は F A X端末に限定されるものではなく、例えば、メール端末も使用することができる。なお、受注センタがインターネットと結合し、メール端末を使用する多数のユーザからの受注処理を行なうような場合においては、とくに発注者および発注確認者のなりすまし防止の観点から、本発明の手書き署名による個人特定または登録者証明機能が必須となろう。

【0065】《情報提供通信システム（ビデオテックス）》加入者端末から公衆網経由で情報センタに接続し、利用者の要求に応じて文・図形等の画像情報を提供するシステムとして、ビデオテックス通信システムがある。最近では、パソコンやインターネット利用への普及をめざしたサービス展開による情報提供通信システムとして、利用者に競馬情報、カラオケ・楽曲データ、その

他の有料情報を提供するシステムが構築されている。このような情報提供通信システムでは、情報提供者への利用料金の回収、情報利用者の特定や情報利用者への請求金の回収などについて、通信システム内での自動的な処理が実現できるが（例えば特願平 9-230093 号）、本発明の手書き認証通信システムを適用することにより、簡単な構成であって、かつよりセキュアな情報提供通信システムとすることができる。

【0066】（システム構成）図 10 は、本発明の手書き認証通信システムを適用した情報提供通信システムの構成を示すブロック図である。この情報提供通信システムは、競馬情報、カラオケ・楽曲データ、その他の有料情報を提供する装置として機能する不特定多数の情報サーバ 61 と有料情報にアクセスする多数の端末装置 62 とが、サービス提供網（公衆網）63 及びインターネット 64 に接続するとともに、サービス提供網 63 に課金回収代行サーバ群 65 と手書き認証サーバ 66 を接続したものである。各端末装置 62 には、図 3 に示すものと同様の手書き入力装置 23 が接続している。手書き認証サーバ 66 としては、図 2 に示し、また上述の各手書き認証通信システムで説明したものと同様のものが、使用される。サービス提供網 63 とインターネット 64 とは、図示しないゲートウェイを介して接続している。

【0067】課金回収サーバ手段である課金回収代行サーバ群 65 は、課金処理サーバ 67、請求処理サーバ 68 および回収処理サーバ 69 からなっている。課金処理サーバ 67 は、有料情報の格納先アドレスを保持しており、利用者の端末装置 62 からの情報要求に対応する情報サーバ 61 を特定し、有料情報の利用に対して課金すべき金額情報を情報サーバ 61 から取得するとともに、有料情報を端末装置 62 に代理送信し、金額情報により課金額を決定し、決定した課金額を利用者ごとに情報蓄積を行なうとともに、請求処理サーバ 68 に対して課金通知を行なうものである。請求処理サーバ 68 は、課金処理サーバ 67 で決定された利用者ごとの課金額の累計額と、図示しない電話料金管理機関側の料金管理システムでの公衆回線使用額と、を統合して請求処理を実行するものである。また、回収処理サーバ 69 は、利用者から金融機関への料金振込情報に基づいて回収額を情報提供者ごとに集計し、情報提供者の I D や振込口座番号を特定し、その口座に料金を振り込む処理を行なうものである。

【0068】この情報提供通信システムは、インターネット上で一般的な無料閲覧とは異なり、有料情報の閲覧を実現するシステムであり、情報提供者への正確な料金回収と情報利用者の正確な個人の認識、特定が要求される。このため、情報利用者のユーザ I D とともに、利用者特定のための手書き署名による認証プロセスを設けたものである。

【0069】（処理手順）基本的な処理手順は、情報利

【 0 0 7 2 】（情報利用手順）情報の提供を受けようとするとき情報利用者は、まず、情報利用者の端末装置 6 2 においてユーザ I D、パスワードならびに情報提供先アドレスを入力するとともに、手書き入力装置 2 3 で手書き署名を行なってこれを添付ファイルとし、情報利用要求を送信することによって、情報提供通信システムにアクセスする。この情報利用要求は課金処理サーバ 6 7 によって受け付けられ、課金処理サーバ 6 7 は、ユーザ I D およびパスワードにより加入契約登録の有無を判断した後、手書き認証サーバ 6 6 に情報利用者個人のユーザ I D と手書き署名データファイルとを転送する。これにより、手書き認証サーバ 6 6 は、手書き署名の認証を行ない、判定結果を課金処理サーバ 6 7 に送信する。

【 0 0 7 9 】（システム構成）図 1 2 は、公的証明配送通信システムの構成を示している。そのシステムでは、公衆網 1 3 あるいはインターネット 1 1 に、手書き署名を入力するための手書き入力装置が結合した F A X 端末 2 1 やメール端末 2 2 が接続されており、通信網側には、各種機能処理用の F A X サーバ 3 1、サービス制御

サーバ 33、加入者管理サーバ 34、手書き認証サーバ 36 及び課金回収サーバ群 37 が分散配置されている。FAXサーバ 31、サービス制御サーバ 33、加入者管理サーバ 34 及び手書き認証サーバ 36 としては、上述した手書き認証通信システムにおけるものと同様のものが使用され、また、課金回収サーバ手段である課金回収サーバ群 37 としては、上述の情報提供通信システムにおける課金回収代行サーバ群と同様のものが使用される。市役所などの公的機関 44 では専用の LAN 42 が構築されており、この LAN 42 は、専用線 40 を介して公衆通信網側に接続している。公的機関 44 の LAN 42 には多数の FAX 端末 21 及び PC 端末 24 が接続するとともに、住民台帳、戸籍台帳等の多大な個人情報

を蓄積したデータベース (DB) 43 と、LAN 42 内外との処理を行なう PC サーバ 41 が設置されている。PC サーバ 41 は、用途や規模に応じて複数配置される。また、各 PC 端末 24、各 FAX 端末 32 には手書き署名入力用の手書き入力装置 23 が接続されている。

【0080】このような構成の公的証明配送通信システムにおける公衆通信網側での各種サーバに関して説明すれば、上述したように、課金回収サーバ群 37 は、証明書等の交付手数料等の収受を行なう機能を有し、手書き認証サーバ 36 は、各種公的証明書等の交付請求での本人認証を行なう機能を有する。つまり、この公的証明配送通信システムは、公的証明の請求処理を上述の受発注通信システムで行ない、手数料等の徴収処理を上述の情報提供通信システムで行ない、その間の本人認証を手書き署名データの送受信により処理するという、統合的な通信システムである。

【0081】(処理手順) この公的証明配送通信システムにおける基本的な通信処理手順は、以下のステップからなる。

(ステップ 1) 請求者側の端末からの公的証明書等の請求要求:

(ステップ 2) 公衆通信網側による請求文書の送信:

(ステップ 3) 公的機関からの公的証明請求書書式の送信:

(ステップ 4) 公的証明請求書への記載・送信、手書き署名データの送信:

(ステップ 5) 公衆通信網側での請求者の本人認証、認証結果の通知:

(ステップ 6) 公的機関での証明書等の交付と手数料金の照会・明示処理:

(ステップ 7) 公衆網側での交付担当者の認証、請求者の支払い口座の確認

(ステップ 8) 請求者への公的証明書の発送、手数料請求の承認:

(ステップ 9) 手数料支払い者の認証通知、公的機関への手数料の支払い通知。

この公的証明配送通信システムでの具体的な処理手順を

図 13 及び図 14 に示す。

【0082】公的証明等の請求者は、手書き署名データを事前に手書き認証サーバ 36 に登録しておくものとする。また、公衆通信網側では、請求者の電話や FAX 番号、通話料金支払い口座番号等の情報を蓄積しておくものとする。

【0083】まず、公的証明書等の請求者は、公衆網 13 側あるいはインターネット 11 側の端末 (FAX 端末 21 あるいはメール端末 22) から、住民票や印鑑証明等の請求要求を市役所等の公的機関宛に送信する。ここでは、請求者が FAX 端末 22 を用いて請求要求を発するものとする。この請求要求は、送信要求として、FAX サーバ 31 によってまず受け付けられてサービス制御サーバ 33 に送られる。サービス制御サーバ 33 は、加入者管理サーバ 34 にアクセスすることによって照合処理 (発照合要求と発照合応答) を行ない、FAX サーバ 31 に対し、請求画情報要求を送信するように要求する。これを受けて FAX サーバ 31 は、請求画情報要求を公的機関 44 側に送信する。

【0084】公的機関 44 では、請求画情報要求は、PC サーバ 41 のうち本人認証を行うもので受け付けられ、そこで、登録者の有無が確認され、その後、請求画情報要求は請求書配送のサーバに転送され、この請求書配送のサーバから、証明書の請求伝票 (交付請求書) に相当する請求画情報が FAX サーバ 31 を介して FAX 端末 21 に送られる。ここでは、PC サーバ 41 での自動処理により、登録者の有無の確認と請求画情報の配送を行うものとしたが、本人認証を手で行うことも可能である。その場合には、請求画情報要求を請求受理用の FAX 端末 21 で出力し、手で登録者の有無を確認した後、ファクシミリ送信によって、請求伝票と所定の箇所に必要事項を記載するように案内する案内文とを請求者に返信する。

【0085】次に、請求者は、請求伝票に必要事項を記載した後、手書き署名を行ない、添付ファイルとして送信する。上述の各通信システムにおけるものと同様の処理フローにより請求者の手書き署名を認証したのち、サービス制御サーバ 33 は、公的機関 44 には認証結果通知を送信し、FAX サーバ 31 には記入済み書式 (返信画情報) の送信を要求する。FAX サーバ 31 は、返信画情報を公的機関 44 に送信する。返信画情報は、PC サーバ 41 のうち請求書配送サーバに受け付けられる。

【0086】公的機関 44 では公衆網側での認証通知を本人認証サーバにおいて確認し、その確認の結果を請求書配送サーバに転送し、請求書配送サーバは、手数料請求サーバに対して手数料の照会を行なうとともに、公的証明文書と公的機関 44 での担当者の手書き署名データとをサービス制御サーバ 33 に送信する。また、公的機関 44 の手数料請求サーバは、手数料請求データをサービス制御サーバ 33 に送信する。



【0087】公衆通信網側では、サービス制御サーバ33が、手数料請求に基づいて課金回収サーバ群37に課金処理を要求し、課金回収サーバ群37から、請求者の通話料支払い開設口座番号、端末番号、手数料等の情報を収集する、同時に、公的機関担当者の手書き署名データを手書き認証サーバ36に送信し、その認証結果を得る。その後、サービス制御サーバ33は、FAXサーバ31を介して手数料請求要求と公的証明文書とを請求者のFAX端末21に送信する。

【0088】請求者は公的証明文書を受信するとともに、手数料の徴収を承認するために手数料請求書に手書き署名を行ない、手書き署名データを送信する。手書き認証サーバ36からの手書き署名データによる認証結果の通知により、サービス制御サーバ33は、FAX端末21側へは完了通知を送信し、課金回収サーバ群37に対しては手数料の課金処理を依頼し、課金処理応答を待って、公的機関44の手数料請求サーバに手数料の徴収を通知する。

【0089】以上説明した公的証明配送通信システムでは、本人認証を通信システム側で行なってその認証結果を相手側に通知したりシステム内部への蓄積情報として活用することにより、他人による公的証明請求のなりすましが防止できるとともに、公的証明発行側での担当者の認証による手数料請求・徴収の適否の情報蓄積、請求者への手数料徴収の承認等が一貫して処理できる。このため、複数の公的機関で独立に個人認証処理装置を設ける必要がなくなり、公的機関への多様なアクセスが通信システムにより処理できるようになる。

【0090】

【発明の効果】以上説明したように本発明では、公衆通信網内に手書き認証サーバを設置するとともに、FAX端末やメール端末などの入力端末には手書き署名データ投入用の手書き入力装置を接続することにより、メール通信、ファクシミリ通信、有料情報提供通信あるいは受発注通信などの多様な通信時に、入力端末からのパスワードによる判別ではなく、手書き署名データの判別により、情報アクセス者の特定を行なう。これにより、本発明によれば、情報アクセス者本人の手書き署名データについて事前登録ファイルとアクセス時点でのファイルの同一性による動的署名照合をおこなう通信システムを提供できる。

【0091】また本発明では、入力端末に手書き入力装置を接続し、公衆通信網内に手書き認証サーバとサービス制御サーバを設置することにより、公衆通信システムにおいて情報アクセス者が事前登録者であるかどうかの判定を行ない、認証結果を通知できるため、各種の個別通信システム内に認証機能を配置する必要がなくなる。このため、通信システムの提供と個人認証を一体化して多様な通信システムを構築可能となった。さらに、手書き署名データが個別通信システムには送られることがな

いので、故意または不注意による手書き署名データの流出を防ぐことができ、セキュリティが向上する。

【0092】さらに本発明は、第三者認証証明機関での公開鍵暗号方式を応用したデジタルID認証方式とは異なり、事前に登録された個人本人の手書き署名により認証する動的署名照合であるため、秘密鍵の保存や公開鍵の取得等の繁雑さが無い。

【0093】本発明の手書き認証通信システムを受発注システムに適用した場合、発注元の店舗単位でなく個人単位で発注者や発注確認者の特定が可能になる。

【0094】本発明の手書き認証通信システムを情報提供通信システムに適用した場合、利用者の特定がより明確になるとともに、課金処理までを一括して行うことができ、さらに、端末単位でなく個人単位での課金処理が可能になる。

【0095】本発明の手書き認証通信システムを公的証明通信システムに適用した場合、他人による公的証明請求のなりすましが防止できるとともに、公的証明発行側での担当者の認証の正当性を請求者側が確認でき、さらに手数料請求・徴収の適否の情報蓄積、請求者への手数料徴収の承認等が一貫して処理できるようになる。

【図面の簡単な説明】

【図1】本発明の実施の一形態の手書き認証通信システムの構成を示すブロック図である。

【図2】手書き認証サーバの構成を示すブロック図である。

【図3】手書き入力装置の構成を示すブロック図である。

【図4】電子メール入力による初期登録処理の流れを示す図である。

【図5】初期登録用のメールにおける指定例を示す図である。

【図6】画情報の送受信処理の流れを示す図である。

【図7】受信画情報に対する認証結果の通知例を示す図である。

【図8】本発明に基づく認証機能付受発注情報処理システムの構成を示すブロック図である。

【図9】図8に示す受発注情報処理システムでの基本的な処理の流れを示す図である。

【図10】本発明に基づく情報提供通信システムの構成を示すブロック図である。

【図11】図10に示す情報提供通信システムでの処理の流れを示す図である。

【図12】本発明に基づく公的証明通信システムの構成を示すブロック図である。

【図13】図12に示す公的証明通信システムの処理の流れを示す図である。

【図14】図12に示す公的証明通信システムの処理の流れを示す図であって、図13に示す以降の処理を示す図である。



【図15】従来のファクシミリ通信システムの構成を示すブロック図である。

【図16】従来のファクシミリ通信システムにおけるメール端末からファクシミリ（FAX）端末への送信処理手順を示すシーケンス図である。

【符号の説明】

11, 64 インターネット

12 中継網

13 公衆網

21 FAX端末

22 メール端末

23 手書き入力端末

30 バックボーン網

31 FAXサーバ（FSV）

32 メールサーバ（MLS）

33 サービス制御サーバ（SVC）

34 加入者管理サーバ（SBMS）

35 変換サーバ（TSV）

36, 66 手書き認証サーバ（TNS）

37 課金回収サーバ群（KSG）

40 専用線

41 PCサーバ

42 LAN

43 データベース

44 公的機関

51 サービス制御サーバインターフェース部

52 認証要求部

53 認証部

54 手書き署名データベース部

10 55 インターフェース部

56 認識データ処理部

57 手書き要素解析部

58 手書き入力パッド

61 情報サーバ

62 端末装置

63 サービス提供網

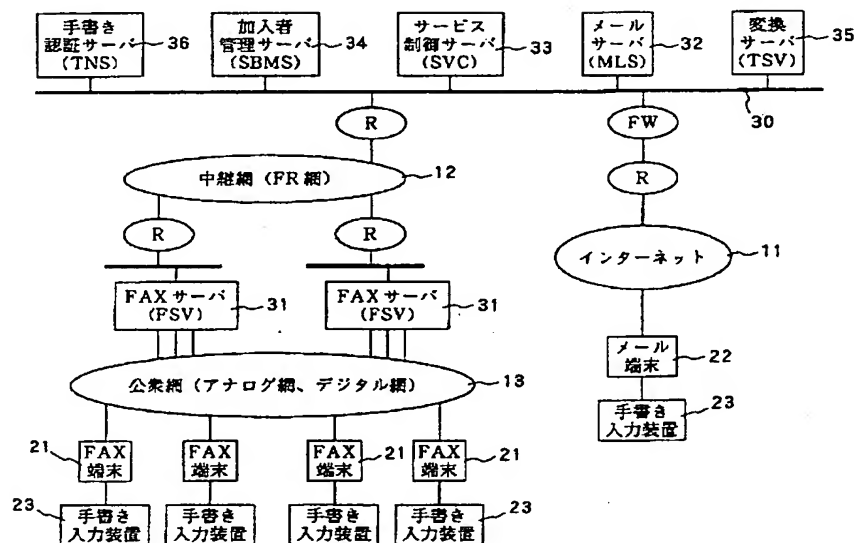
65 課金回収代行サーバ群

FW ファイアウォール

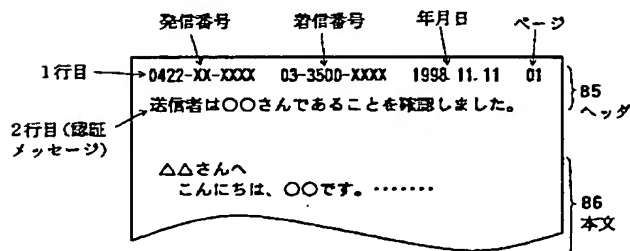
R ルータ

20

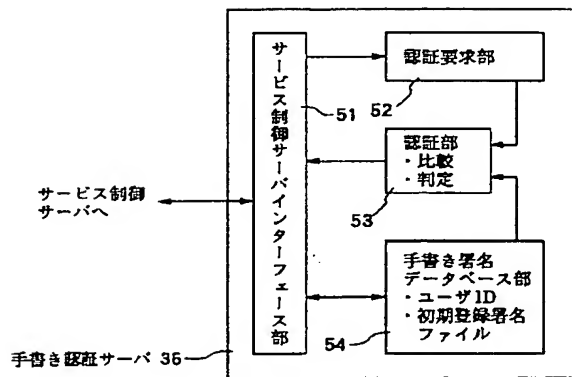
【図1】



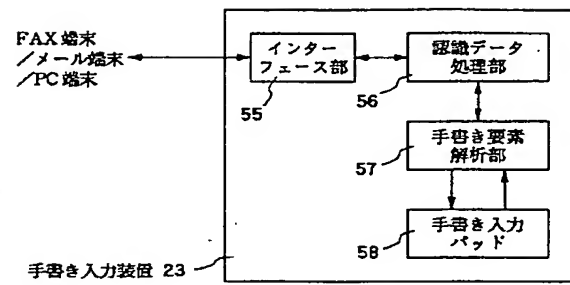
【図7】



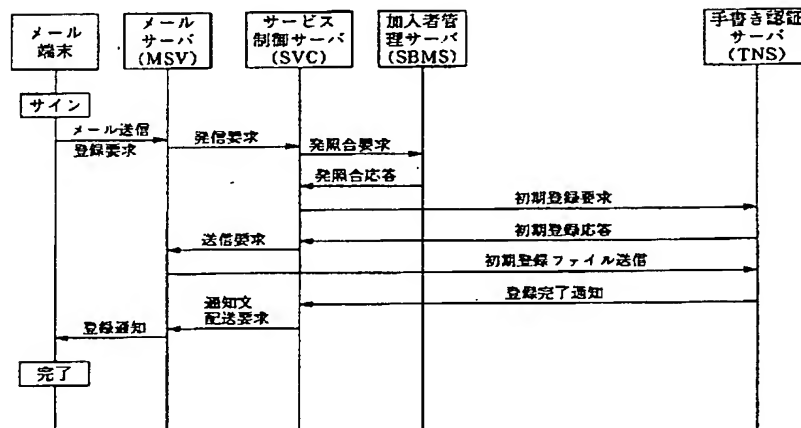
【図2】



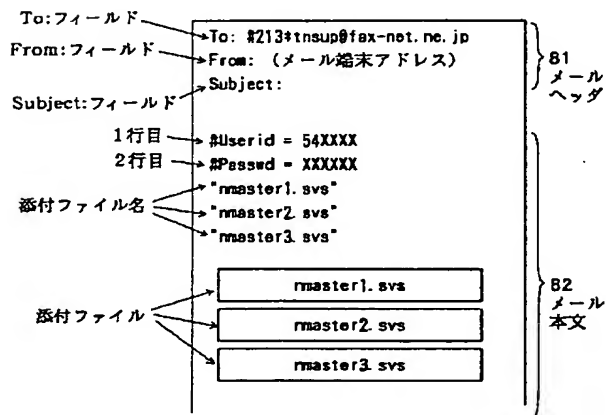
【図3】



【図4】



【図5】



```

sequenceDiagram
    participant ME as メール端末
    participant MSV as メールサーバ(MSV)
    participant SVC as サービス制御サーバ(SVC)
    participant SBMS as 加入者管理サーバ(SBMS)
    participant TNS as 手書き認証サーバ(TNS)
    participant FSV as FAXサーバ(FSV)
    participant FE as FAX端末

    Note over ME: 画情報+サイン
    ME->>MSV: メール送信  
手書き署名ファイル
    MSV->>SVC: 発信要求
    SVC->>SBMS: 発照合要求
    SBMS-->>SVC: 発照合応答
    SVC->>TNS: 認証要求
    TNS-->>SVC: 認証応答
    SVC->>MSV: 署名ファイル送信要求
    MSV->>TNS: 署名ファイル送信
    TNS->>SVC: 認証結果通知
    SVC->>ME: 画情報送信要求
    ME->>SVC: 画情報送信
    SVC->>FE: 認証結果通知
    FE->>FSV: 画情報送信
    FSV->>FE: 認証結果送信
    FE->>SVC: 受信完了通知
    SVC->>SBMS: 通知文作成要求
    SBMS-->>SVC: 通知文作成
    SVC->>ME: 通知文作成
    ME->>ME: 完了

```

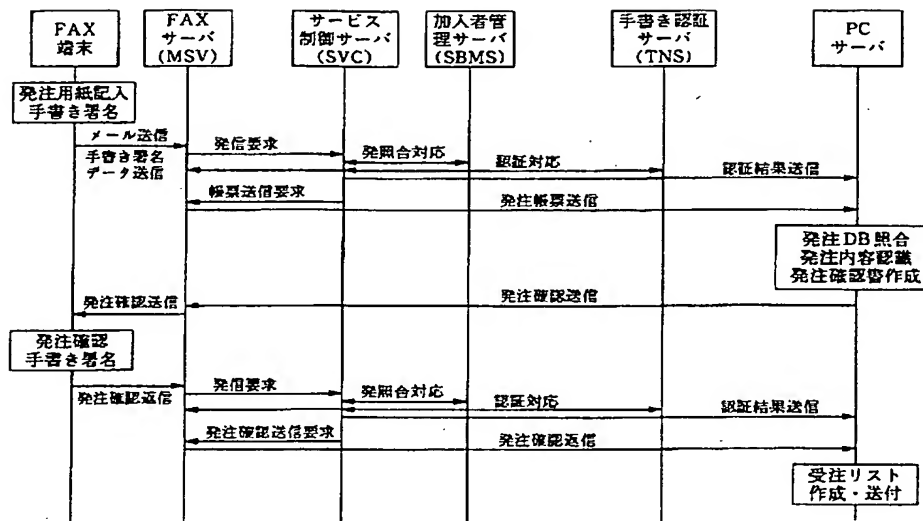
```

sequenceDiagram
    participant FAX as FAX 端末
    participant MSV as FAX サーバ (MSV)
    participant SVC as サービス 制御サーバ (SVC)
    participant SBMS as 加入者管理サーバ (SBMS)
    participant TNS as 手書き認証サーバ (TNS)
    participant KSG as 課金回収サーバ群 (KSG)
    participant 本人 as 本人 認証
    participant 請求 as 請求書 配送
    participant 請求 as 手数料 請求

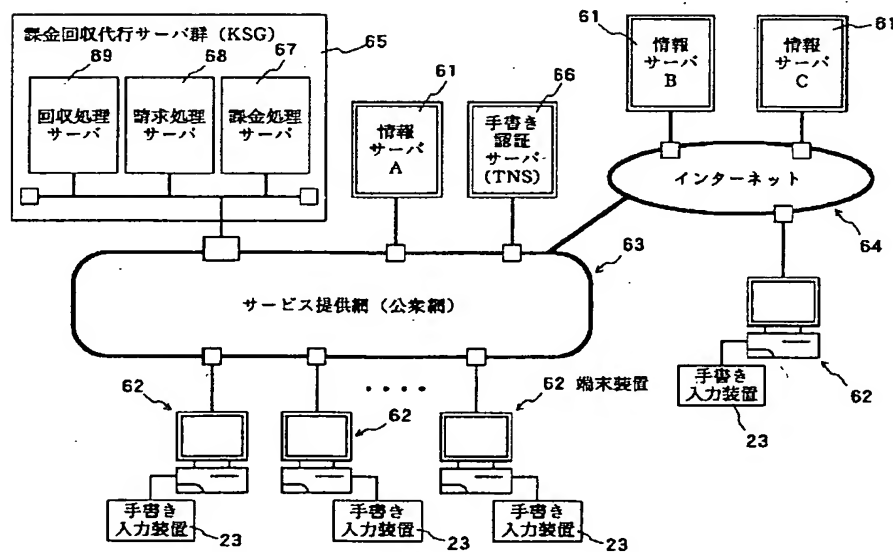
    FAX->>MSV: 
    MSV->>SVC: 承認送信
    SVC->>SBMS: 手書き署名データ送信
    SBMS->>TNS: 認証応答
    TNS->>KSG: 手数料課金処理
    KSG->>本人: 手数料課金処理応答
    本人->>請求: 手数料量収通知
    請求->>請求: 
    請求->>請求: 
    
```

The diagram illustrates the payment processing flow. It starts with a FAX terminal sending data to a FAX server (MSV). The MSV sends an approval message to a service control server (SVC). The SVC then sends handwritten signature data to a subscriber management server (SBMS). The SBMS sends an authentication response to a handwritten authentication server (TNS). The TNS sends a fee and billing processing message to a billing recovery server group (KSG). The KSG sends a fee and billing processing response to the user (本人). Finally, the user sends a fee and billing amount notification to the billing recovery server group (KSG). The KSG then sends a request for a bill to the billing recovery server group (請求書 配送) and a request for a fee (手数料 請求).

【図9】



【図10】



```

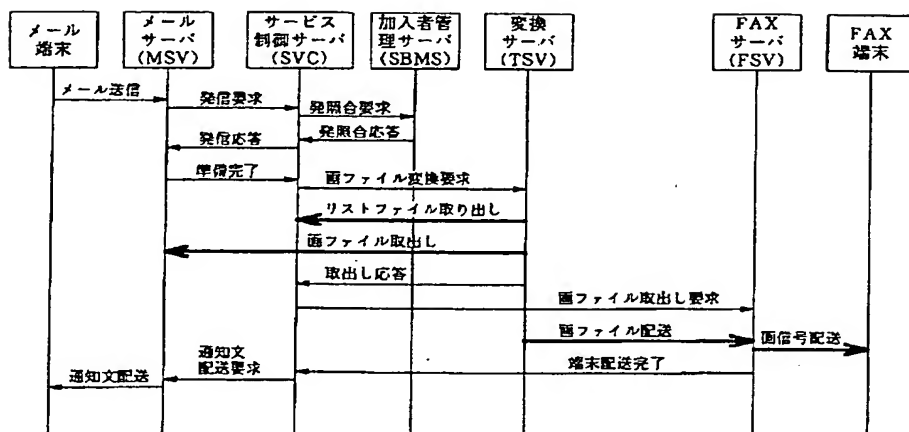
sequenceDiagram
    participant ILE as 情報利用  
端末
    participant DLE as 課金処理  
サーバ
    participant RLE as 請求処理  
サーバ
    participant HLE as 回収処理  
サーバ
    participant HSE as 手書き認証  
サーバ
    participant ISE as 情報  
サーバ
    participant KMS as 料金管理  
システム

    ILE->>ILE: 初期登録
    ILE->>ILE: サイン
    ILE->>DLE: 初期登録要求
    DLE->>RLE: 初期登録要求
    RLE->>HLE: 初期登録応答
    HLE->>DLE: 初期登録ファイル送信
    DLE->>ILE: 登録通知
    RLE->>HLE: 登録完了通知
    ILE->>ILE: 情報利用
    ILE->>ILE: サイン
    ILE->>DLE: 情報利用要求
    DLE->>RLE: 情報利用者認証要求  
(ユーザID + 手書き署名ファイル)
    RLE->>HSE: 判定結果送信
    HSE->>DLE: 情報利用要求
    DLE->>ISE: 情報データ + 課金情報送信
    ISE->>ILE: 情報代理  
提供
    DLE->>RLE: 課金結果通知
    RLE->>HLE: 課金結果通知
    HLE->>DLE: 公衆回線使用額通知
    DLE->>KMS: 情報利用者、情報提供者への課金通知
    KMS->>HLE: 回収額通知
    HLE->>HLE: 回収額通知
  
```

[illegible]



【図 16】



フロントページの続き

(51) Int. Cl.<sup>7</sup> 識別記号 F I テーマコード (参考)  
 H04N 1/00 107 G06F 15/62 465 P 5K101

Fターム(参考) 5B043 AA05 BA06 CA09 DA07 EA06  
 GA02 HA20  
 5B085 AC04 AE23 AE25 BG07  
 5B089 GA02 GA11 GA21 GA26 HA01  
 JA05 JB03 JB22 KA17 KB13  
 KC47 KC58  
 5C062 AA02 AA10 AA14 AA27 AA30  
 AA32 AA35 AB18 AC22 AC28  
 AC43 AE02 AE08 AE14 AF08  
 AF12 BC05 BD06  
 5K025 AA01 BB02 BB10 CC01 EE18  
 5K101 KK01 NN01 NN18 NN21 PP04  
 TT06